

2131 #4

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of: PAUL PERE :
Serial No. 09/701,790 :
Filed: June 2, 1999 :
For: METHOD FOR SECURED ACCESS TO:
DATA IN A NETWORK :



TRANSMITTAL OF SUBSTITUTE SPECIFICATION

RECEIVED
FEB 27 2001
Group 2100


Hon. Commissioner of Patents
and Trademarks
Washington D.C. 20231

Sir:

Transmitted herewith is a Substitute Specification.
This application has been prepared to facilitate examination by
reformatting the literal English language translation of the
International application into U.S. form and clarifying the
language of that translation.

The substitute specification submitted contains no new
matter.

Respectfully submitted,


Elliott N. Kramsky
Reg. No. 27,812
Attorney for Applicant

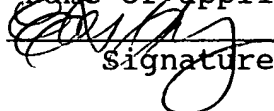
(818) 992-5221

I hereby certify that this correspondence is being
deposited with the United States Postal Service
as first class mail in an envelope addressed to:
Assistant Commissioner for Patents,
Washington, DC 20231, on 2/20/01

(Date of Deposit)

Elliott N. Kramsky Reg. No. 27,812

Name of applicant, assignee, or Registered Rep.


Signature

2/20/01
Date

SUBSTITUTE SPECIFICATION



Title: METHOD FOR SECURED ACCESS TO DATA IN A NETWORK

Inventor: Paul Pere

BACKGROUND

RECEIVED
FEB 27 2001
Group 2100

5 Field of the Invention

The present invention relates to a method for secured access to data in a network of the type that includes an information center and at least one data area access system (a device which provides storage space (data area) and permits access to stored data).

10 Description of the Prior Art

In the near future, "networks of practices" will be developed for different interest groups of a public or private nature (e.g., in health care, sickness insurance agencies, the health ministry and medical associations). The basic idea of these networks of practices is that, on the basis of better communication between different doctors' practices and/or hospitals, the number of often-redundant medical examinations currently carried out may be reduced. As an example, it would not be necessary to produce a further X-ray image of a lung of a patient if renewed diagnosis (e.g., by a different doctor) were possible with the assistance of an easily accessible, recently

taken X-ray image of the patient's lung. It is in the public interest and that of insurance companies to reduce health costs. For this reason, the latter, in particular, would like to set up autonomous medical networks with the aid of which a patient's different doctors can access data already prepared by their colleagues to thus provide the patient with better and more cost-effective medical care.

In established test models, the main problem is that of ensuring secure communication. There are different known ways of connecting a doctor to medical units, mainly restricted to a certain group of doctors (e.g., radiologists), with a restriction to a specific type of information/data, for example X-ray plates, being prescribed.

Some national and international standards that define the way in which medical data are generated and transmitted already exist (e.g., DICOM for X-ray plates, BDT for the data of a patient, GDT for medical data generated by medical equipment such as an electrocardiograph or other devices). No special requirements have to be met in these cases with regard to the secured transmission of medical data as this is no longer a problem today on account of various known encryption mechanisms.

One particular task in the transmission of medical data is to safeguard the rights to personal privacy of the patient. Currently, the transmission of medical information is always illegal whenever it is not restricted to a closed medical group such as a hospital or a doctor's practice. To describe a network of practices with hundreds of different practices and hospitals as a closed group would probably have to be interpreted in the legal sense as an evasion of the patient's personal rights. In this case, a patient would have no possibility of knowing all the members of the group and could scarcely make use of his right to select a different group (e.g., a different hospital).

SUMMARY AND OBJECTS OF THE INVENTION

It is therefore the object of the invention to specify a method for secured access to data in a network, in which only the owner of the rights to the data can define, modify or withdraw access rights of third parties to the data.

The present invention addresses the preceding and other objects by providing a method for secured access to data in a network including an information center and a plurality of data area access systems in which permission to store and define access rights of third parties to data at the information center are limited to the owner of rights to the data to be stored. The method is begun by, in each case, storing data only once in one

of the data area access systems not accessible to the owner of the rights. The presence of data of a certain type in each data area access system is registered at the information center. This is followed by the owner, should he wish, defining access rights of third parties to the data at the information center.

A list of the data present of a certain type, specifying the data area access system storing the data, is transmitted from the information center to a requesting data area access system for which the access rights of the requesting data area access system correspond to the access rights defined at the information center for such data. This occurs after a request of a requesting data area access system for data of such certain type.

The data of the certain type is then directly transmitted by the data area access system storing such data to the requesting data area access system subject to such data area access system storing the data having received a confirmation from the information center.

The method according to the invention provides that only the owner of the rights to certain data can define access rights to these data. Once stored, the data remain where they are stored and are not gathered at a central location. Access to

such stored data is possible only with the authorization of the owner of the rights to these data. For medical data, this means, for example, that they remain at the place where they are prepared and that other doctors can access these data only with the permission of the respective patient. Such permission can be granted generally for certain doctors or else granted only for the individual case.

It is also possible to withdraw permission again once it has been granted.

The preceding and other features of the invention will be further appreciated by the detailed description that follows. Such description is accompanied by a set of drawing figures. Numerals of the drawing figures, corresponding to those of the written description, point to the various features of the invention with like numerals referring to like features throughout both the drawing figures and the written description.

BRIEF DESCRIPTION OF THE DRAWINGS

Figure 1 illustrates a network for employing the method of the invention;

Figure 2 illustrates the generation and storage of data in accordance with the method of the invention;

Figure 3 illustrates an unsuccessful request for data;

Figure 4 illustrates the retrieval and granting of access rights to certain data by the owner of the rights to such data; and

5 Figure 5 illustrates a successful request for data and their transmission to the requesting location.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENT

The method according to the invention is explained below, taking a network of practices as an example. Here, the system
10 serves to provide a group of doctors with the medical records of their patients. The system can be accessed by a number of doctors, each having access to a data area access system. In addition to the data area access systems, the system has an information center. For the sake of simplicity, in figure 1 this
15 system is shown with only two data area access systems 1, 2, one of which has an identification DRZS1 and the other DRZS2. Such a data area access system 1, 2 may be set up at the premises of one or more doctors. For example, it is shown in Figure 1 that the data area access system 2 is set up at a practice of a doctor B
20 and the data area access system 1 is set up at a hospital in which a doctor A has access authorization. Each data area access system 1, 2 can communicate via a network 4 with an information

center 3 or another data area access system 1, 2.

Each data area access system 1, 2 contains a secure data memory for storing the medical data of patients. The memory is access-secured by data access that takes place only by means of the method of the invention. As a result, misuse of data stored in the memory is not possible. Furthermore, it is insured by the invention that only new data can be stored (i.e., data which have not already been stored in another data area access system 1, 2). Furthermore, both the doctor and the patient can communicate independently of each other via the data area access system 1, 2 with the information center 3 or another data area access system 1, 2 connected to the network 4, with only one doctor being able to store data.

In the information center 3, references to the data of the patients and the associated identification information of the patients and doctors are stored at a central location. The security of the individual data transmissions within the system is insured by encryption of the data transmissions between all participants. This involves each item of information transmitted within the system being provided with a digital signature. In the case of every access, authorization is demanded, and all data are transmitted and stored in encrypted form. Each participant (e.g., a doctor or a patient), as well as the information center,

and each data area access system have two pairs of public and secret codes for data encoding. One pair of such codes, known as the encryption codes, is used for the secure data transmission and the other (the signature codes) provides the transmitted information with a digital signature and thereby confirms the sender. The secret codes are known only to the respective participant, information center or data area access system. In contrast, the public codes are accessible to all participants (i.e. every participant in the system can obtain a public code of any other participant). Whenever a participant sends an item of information over the network, the following method is performed:

1. The sender provides the item of information sent by him with a digital signature by using his secret signature code. As a result, the sender cannot be imitated and the recipient is able, with the aid of the public signature code, to confirm the digital signature employed. If, for example, a data area access system sends the patient information to the information center, such information must also be encrypted with the secret signature code of the patient when the data are generated. This assures that the information really does belong to the named patient and that the patient agrees to the transmission of this information.

2. The sender encrypts all transmitted data by means

of a public encryption code of the recipient to whom the data are being transmitted. As a result, the transmitted data can be decrypted only using the secret encryption code of the recipient.

3. Whenever a participant accesses the system, he must be authorized and have his identity confirmed. A special data carrier, such as a smart card, may serve for transmitting the identity of the participant. Of course, other methods of personal identification may also be used, such as voice recognition, image recognition, fingerprint recognition, etc., which can be used individually or in combination.

A special data carrier, such as a smart card, may be used as a secure memory for the secret codes of a participant and other personal information. The public codes of the participants, the information center 3 and the individual data area access systems 1, 2 may be stored centrally at the information center 3.

Figure 2 illustrates the generation of data of a patient and the procedure by which such data are made available in the system. The patient N visits the doctor A on a day X and has a new medical data unit (e.g., an X-ray image) prepared. If the patient N desires, this data unit can be made available to other doctors over the network of practices. In this case, in a first step S1, the data of the X-ray image are stored in electronic form, together

with an electronic form that includes the type of the data, in the data area access system 1 with the identification DRZS1 of the doctor A. The type of data in this case comprises information that it is an X-ray image of the patient N, which the doctor A took on day X. It is also possible for the type of data to comprise only one of these items of information, or for other information to be added, such as the identification DRZS1 of the data area access system 1 storing the data. The data of the X-ray image are stored together with the electronic form in the secured data memory of the data area access system 1. Storage of data is only possible with authorization of the owner of the rights to these data, which may be accomplished, for example, by the patient's smart card.

In a second step S2, the information center 3 is notified by the data area access system 1 that it has new data, that is an X-ray image of the patient N. Such notification may take place either directly after the storage of the new data or at a certain point in time, for example regularly at a certain time of day. It is also possible for the information center 3 to send inquiries as to whether new data have been stored to each data area access system 1, 2 at certain points in time.

In a third step S3, the information center 3 registers the presence of the X-ray image of the patient N of the day X with the availability in the data area access system 1 and allocates these

data a unique identification (e.g., NXAX), after which such identification is transmitted, with a notifying confirmation, from the information center 3 to the data area access system 1. In the data area access system 1, the identification thus allocated is used for administration of the associated data, in that it is added to these data. It can be insured by an appropriate configuration that data are not replicated in the system. At the latest, when the data are registered by the information center 3, a verification of the authorization for data storage by the patient takes place. In the case of no authorization, access rights to these data are not granted to any participant.

In Figure 2 and the subsequent figures, the hollow arrow signifies a transmission of data into the system (i.e., the storage of new data in a data area access system 1, 2) and the solid arrows signify communications over the network 4 such as a request or notifications. It can consequently be seen from Figure 2 that, in the system described, the medical data are not copied into the information center 3 but always remain in the data area access system 1 after they have been stored. The information center 3 keeps only the references to these data rather than the data themselves. Furthermore, a data transmission via the network 4 is indicated in the figures by means of boxes in which the data transmitted are specified next to solid arrows.

Figure 3 illustrates an attempt to access data via the network of practices. On a day Y, the patient N visits a doctor B, who has a data area access system 2 with the identification DRZS2. This doctor B requires a current X-ray image of the patient N. Therefore, in a step S4, the doctor sends from his data area access system 2 a request for X-ray images of the patient N to the information center 3. The information center 3 prepares a list of references to all X-ray images of the patient N currently present in the system (i.e. stored in any of the connected data area access systems and registered by the information center 3). The information center 3 subsequently verifies the access rights to the data shown in this list with regard to the doctor B from whom the request for X-ray images of the patient N came, and, in a step S5, transmits only the references of the X-ray images of the patient N to which the doctor B has been granted access rights (by the patient N, who in this case is the owner of the rights to his data). Since, in this case, no access rights to his X-ray images have been defined by the patient N, this list is empty. Therefore, the information center 3 sends a message "no data found" to the data area access system 2. The latter outputs this message to the doctor B.

Accordingly, no doctor can identify the data in the system without access rights of the patient who is the owner of the rights to the stored data. It is only possible to break through this

secure system for data for which access rights have been specifically defined if the patient N has, for example, given certain doctors general access rights in advance to all or certain of his data. Even in such a case, however, the patient has
5 determined who can access his data. Here, too, his data protection rights have been respected.

Figure 4 illustrates the definition of access rights of the patient at the information center 3. In step S6, the patient N can retrieve a list of all his data currently available in the system
10 as a whole from the information center 3 via the data area access system 2. Alternatively, he can retrieve only a list of certain data. In a step S7, the information center processes this request and sends the requested list to the data area access system 2. The patient N can now define access rights to the data shown by the
15 list. If, for example, he has requested a list of all his X-ray images, he can define that the doctor B and/or any other doctor or a certain group of doctors can access the X-ray image taken on the day X by the doctor A with the identification NXAX. Such an access right may be for a limited or an unlimited time. The access right
20 may also be granted in advance for the data available in the future. Once the patient N has defined all the desired access rights, he can, in a step S8, bring about an update of the access rights at the information center 3 via the data area access system

2. In a step S9, the information center 3 stores the changes and sends a confirmation back to the data area access system 2.

The access rights may also be granted at the time that new data are being stored in a data area access system 1, 2. A patient or other owner of rights to data stored in a data area access system 1, 2 can grant access rights from any desired data area access system 1, 2. For example, it is conceivable for such data area access systems 1, 2 to be installed not only at doctors' practices or hospitals but also in pharmacies, or for access to a network of practices also to be possible via the Internet whereby every computer capable of being connected to the Internet could become a data area access system or at least an access system that does not provide any storage space. The owner of the rights to data stored in a data area access system 1, 2, (in this case the patient) is the only person who, on the basis of his authorization and identification, can be shown the access rights by the information center 3 and/or can modify them at the information center 3.

Figure 5 illustrates the sequence required for successfully accessing certain data. After the access rights to the X-ray image of the patient N taken on the day X by the doctor A, with the identification NXAX, have been defined by the patient N for the doctor B, the doctor B launches a renewed request to the

information center, in a step S10, to specify all references to the X-ray images of the patient N. In step S11, the information center compiles a list of the references of all the X-ray images of the patient N currently in any of the data area access systems, verifies the access authorizations with regard to the doctor B making the request and selects only the X-ray images which may be accessed by doctor B. It then transmits the associated references to the data area access system 2. In this case only the identification NXAX of the X-ray image of the patient N produced on day X by doctor A is transmitted together with the memory location/address (in this case the data area access system 1 with the identification DRZS1) to the data area access system 2, which displays this information to doctor B. Doctor B can consequently see only the references to the data to which the patient N has granted his access rights. The references may include, for example, the type of data (X-ray image), the date of the examination (day X), the doctor carrying out the examination (doctor A), the memory location of the data (data area access system 1) with the identification DRZS1. In step S12, the doctor B selects the X-ray image with the identification NXAX, whereupon the data area access system 2 sends a request of doctor B for the X-ray image with the identification NXAX to the data area access system with identification DRZS1 (data area access system 1). In step S13, the data area access system 1 sends an inquiry to the information center 3 to confirm that doctor B has the access rights

to the X-ray image with the identification NXAX. The information center 3 replies, in a step S14, with a confirmation, whereupon, in a step S15, the data area access system 1 transmits the data of the X-ray image with the identification NXAX to the data area access system 2. The latter presents the received data of the X-ray image in an acceptable form and/or allows doctor B to store the data for further processing, such storage having to take place not in the secure memory of the data area access system 2 but on another storage medium, since otherwise the data would be replicated in the system.

Once an authorized person has stored the received data for further processing, such person can repeatedly access the stored data. Access via the network of practices is only possible, however, as long as the owner of the rights to these data allows it.

Since the method according to the invention consequently provides that storage of certain data is possible only with the permission of the owner of the rights and retrieval of such data is possible only with the permission of the owner, the personal rights of a patient, for example, are respected. The system operates in an entirely transparent way for any user, without the individual user having to have any knowledge of the security or transmission processes. The encryption of data sent has the effect that

unauthorized persons cannot "listen in" and the definition of certain access rights for certain data by the owner of the rights has the effect that unauthorized access to these data is not possible.

5 When the data are transmitted, it is particularly advantageous if the appropriation specified by the owner of the access rights for the transmission of these data in the original data context is transmitted together with these data in the form of an "electronic watermark" and these data are additionally marked
10 visibly as an appropriated copy of the original data.

 The method of the invention for secured access to data in a network can also be applied to non-medical networks, since a system of controlling the distribution of individual data is proposed. Another area of application is, for example, the
15 distribution of personal data for identification purposes, whereby the transmission of these data between different administrative authorities without a centralized database of individual citizens can be made more flexible. The system according to the invention has the effect that the citizen concerned has sole power of
20 disposal over his personal data.

 While this invention has been described with reference to its presently preferred embodiment, it is not limited thereto.

Rather, the invention is limited only insofar as it is defined by the following set of patent claims and includes within its scope all equivalents thereof.